Cloud Log Monitoring & Threat Detection Lab (with Wazuh or OSSEC)

About the Project

The Cloud Log Monitoring & Threat Detection Lab demonstrates how to monitor, analyze, and detect suspicious login activities on a cloud-hosted Ubuntu server using an open-source SIEM solution — Wazuh (or OSSEC). This project focuses on identifying potential brute-force attacks and unauthorized SSH logins by analyzing system logs in real-time. Through Wazuh's correlation rules and alert dashboard, security incidents are detected and visualized, providing insights into potential threats within a cloud environment.

Objective

To monitor and detect suspicious login behavior (e.g., brute-force or privilege escalation) from a cloud Ubuntu VM using an open-source SIEM agent (Wazuh Agent or OSSEC).

Tools and Environment

Component	Description
Cloud Provider	Oracle Cloud Free Tier or AWS Free Tier
VM 1	Ubuntu Server 22.04 (Wazuh Agent Installed)
VM 2	Wazuh Manager / Attacker VM
Logs Monitored	/var/log/auth.log
SIEM Tool	Wazuh / OSSEC
Ports	22 (SSH), 5601 (Kibana Dashboard)

Methodology

1. Deployed two Ubuntu Cloud VMs (one for Wazuh Manager, one for Wazuh Agent).
2. Installed and configured Wazuh Manager using the official installation script.
3. Installed Wazuh Agent on the monitored VM and connected it to the Manager.
4. Configured monitoring of /var/log/auth.log for SSH login attempts.
5. Simulated multiple failed SSH logins to trigger brute-force detection rules.
6. Verified alerts in the Wazuh dashboard for detection of suspicious activities.
7. Documented findings and incident summary with timestamps and alert details.

Detection Results

Wazuh successfully detected multiple failed SSH login attempts from a simulated attacker host. An alert was generated under rule ID 5710, corresponding to brute-force SSH detection. Subsequently, a successful login alert (rule ID 5712) was observed, indicating a possible compromise scenario. These alerts were displayed in the Kibana-based Wazuh Dashboard, confirming effective log monitoring and detection.

Field	Details
Date/Time	2025-11-13 20:42:13
Event Type	SSH brute-force detected
Source IP	10.0.0.25
Destination VM	Ubuntu Cloud VM (VM1)
Action Taken	Alert raised in Wazuh Dashboard
Evidence	Screenshot of alert and /var/log/auth.log entries

Conclusion

This project successfully demonstrates the deployment of a cloud-based log monitoring and threat detection system using Wazuh SIEM. It effectively detected SSH brute-force attempts and generated real-time alerts for analysis. The setup highlights the importance of proactive log monitoring in maintaining cloud security and improving incident response readiness.